Dave Mitchell dave@singularity-networks.com
www.singularity-networks.com

Singularity Networks

Real-Time Network Analysis
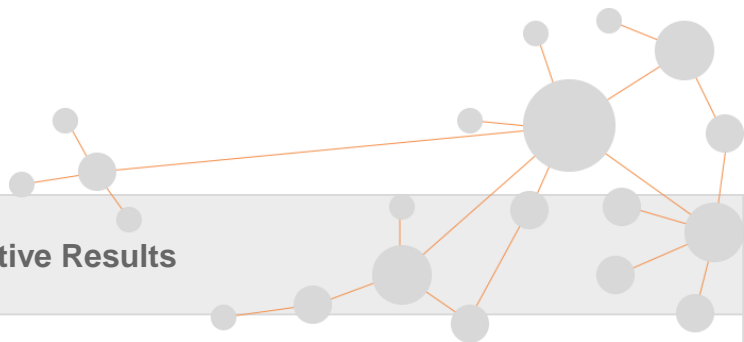
Visualize your network behavior, as it happens

Identify events & anomalies, with detailed context

Respond to issues quickly, with confidence

The Operational Struggle

Current Challenges	Negative Results
Fragmented visibility across hybrid infrastructures	Requires access to multiple interfaces & lacks cohesion
Lack of integration with existing platforms & solutions	Operators cannot make an informed decision, based on correlated data-sets
Data Delay	Outages are unnecessarily prolonged
User interfaces are not configurable, to meet specific requirements	Detailed technical knowledge is required to gain insight
Lack of detail & context, in the data provided	Unable to investigate anomalous network activity, with detailed understanding

How will Singularity help my organization?

Complete Visibility

- Quickly track down the cause of an issue

- Integrate with your current infrastructure, easily

- Reduce lost productivity and customer impact

Security Proficiency is a Side-Effect of Visibility

- Identify traffic that does not adhere to company policy or is anomalous

Proactive Analysis

- Identify potential issues, before they become customer impacting

Compliance & Policy Enforcement

- Configurable rule-based engine, empowering you to immediately detect policy violations

Singularity
NETWORKS

The Singularity Networks Solution

Empowering your organization

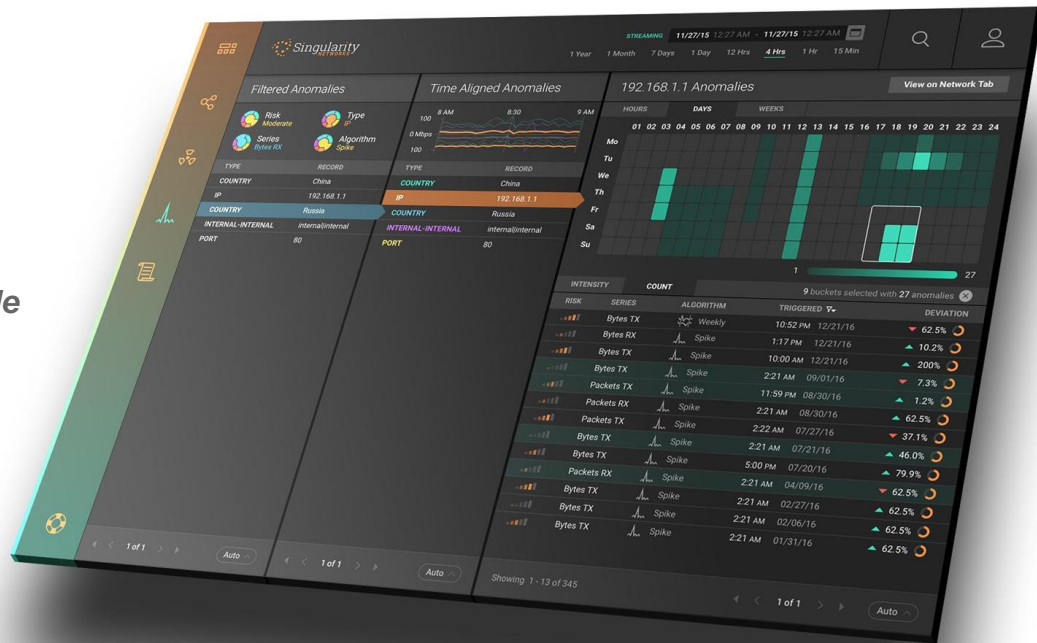### Comprehensive View of Your Network

- Single pane-of-glass to view your corporate network, datacenter and cloud deployments

True Real Time

- Context driven information is *immediately visible* and actionable

Business-Level Insight

- Group traffic by business role
- Visual anomaly analysis
- Assess and forecast cloud deployment costs

Singularity Platform

Highly Configurable Real-time Analytics Platform

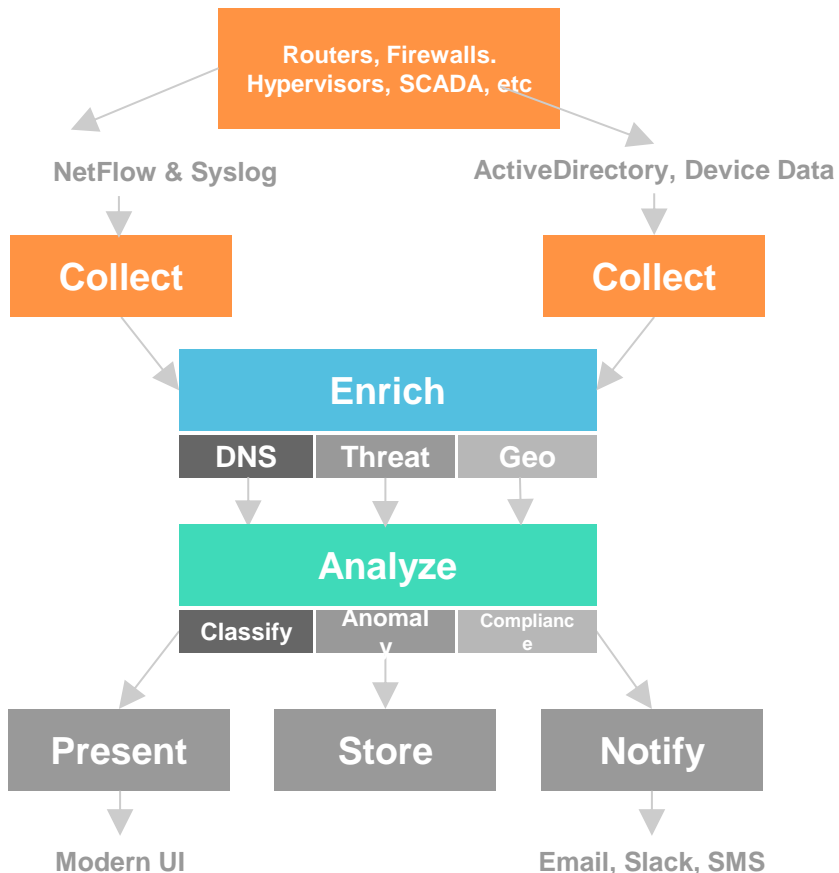**Combine Network Telemetry with Business Context**

- Netflow, Syslog, DNS, BGP, GeoLocation

- Active Directory

- IP Reputation, Whois, NMAP

- Additional data-sets

Classify, Analyze and Alert

- Rule Based Traffic Grouping

- Anomaly Detection

- Policy & Compliance Engine

- Flexible Notifications
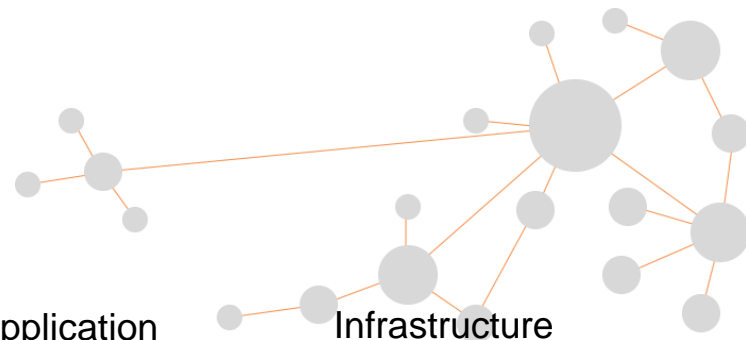
Advanced UI & API

- Advanced Drill Down Capabilities

- Visual Anomaly Analysis

- Streaming API

Routers, Firewalls. Hypervisors, SCADA, etc

NetFlow & Syslog

ActiveDirectory, Device Data

Collect

Collect

Enrich

| DNS | Threat | Geo |

Analyze

| Classify | Anomaly | Compliance |

Present

Store

Notify

Modern UI

Email, Slack, SMS

Singularity NETWORKS

Flexible Integration

Integrate with your current infrastructure, easily

Network

CISCO

JUNIPER NETWORKS

ARISTA

Security

paloalto NETWORKS

radware

FireEye

splunk>

f5

F⌀RTINET

Application

DNS Domain Name System

Apache

NGiNX http server

Infrastructure

Active Directory

Scada

vmware

Singularity NETWORKS

Singularity NETWORKS

Deployment Options

On-premise, Hosted, SaaS & Multi-Tenant

- **Hosted**
  - Netflow, syslog streamed and stored in the cloud
  - **Server probe can generate netflow**
  - SaaS model

- **On-Premise**
  - Installation Options
    - Installed Software - RHEL/CentOS-7
    - Virtual Appliance / Physical Appliance
    - **Multi-tenant capable**
  - Flexible Distributed Model
    - Distribute collectors as needed
    - Separate Database and Analytics for scale
    - Separate security zone for UI
  - Single Server Model
    - Easy to deploy - all processes on one server

Distributed Model

Collector	Collector

Database / Analytics

UI

Single Server Model

Collector
Database / Analytics
UI

Singularity
NETWORKS
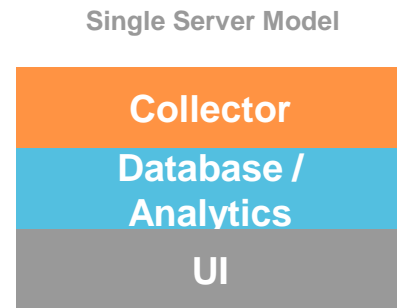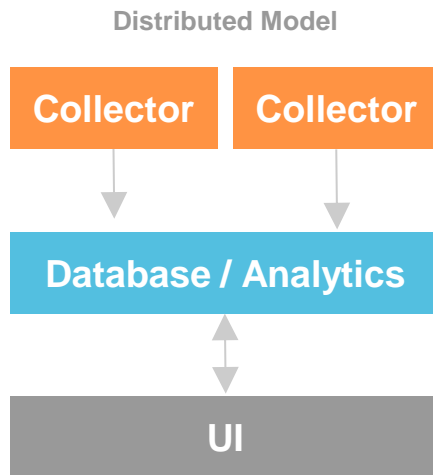
Streaming Analytics Database

Purpose-built, to suit your needs

- **Hardware Efficient Design**

  - Highly Concurrent
    - Linear CPU scaling
  - I/O and Memory Optimized
    - Eliminates store and query I/O bottleneck
    - Solves memory resident DB size limitations
  - Data Aware Storage Methodology
    - Significantly reduces storage requirements
  - Lower TCO vs Traditional Database
    - Reduced hardware footprint
    - Eliminates DB licensing and DBA costs

- **Powerful API**
 - Subscription capability allows data to be immediately propagated upon change

Singularity
NETWORKS

Traditional Big Data Analysis

Design Pattern: Insert, Write, Read, Analyze…

- Each Query Saturates I/O (Read) and CPU (Analyze)

- Analytics Delays from Query Run Time and Inter-Query Spacing

- Insert, Ad-Hoc, and Analytics Compete for IOPS and Bandwidth

Hardware Expansion: Horizontal Scale (More CPU and I/O)

- Large Infrastructure Required (Capital, Power, Cooling, People, etc…)

- **"Real-time":** With Enough Hardware, Measured in Minutes
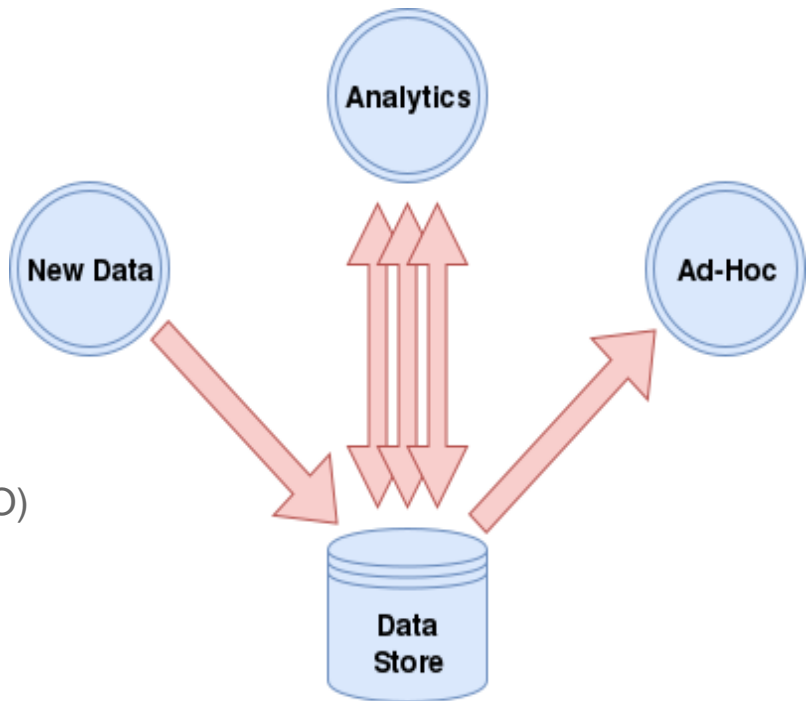
Streaming Analysis Advantage

Design Pattern: Update, Analyze, Write …

- IOPS Become Irrelevant (Analysis Followed by Append)

- Incremental, Continuous Queries Greatly Reduce CPU Cycles

- Disk Bandwidth Preserved for Inserts and Ad-Hoc Queries

Hardware Reduction: Less CPU, Less Disk I/O

- Big Data on Small Hardware (Reduced Cost and Environmental Impact)

- **True Real-time:** New Insights, Second over Second
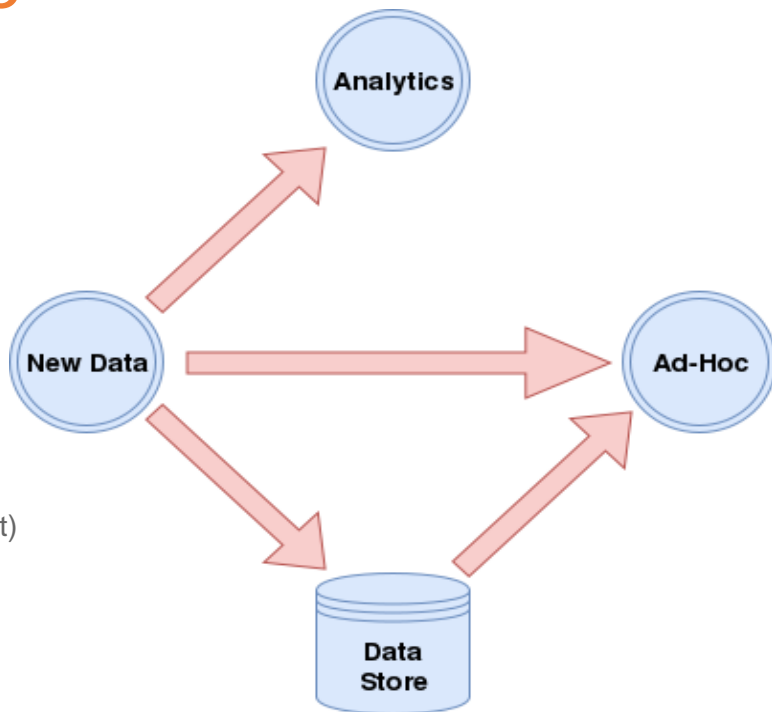
Singularity - API

Singularity utilizes the power of our streaming-based API.

- **WebSocket Based API**
  - WebSocket version 13 (RFC 6455)
  - JSON content
  - TLS encryption enabled by default
  - Token and user/pass authentication supported
  - Standard libraries in Python, Perl and Javascript
  - *UI is 100% built on this API*

- **Command Line Utility**
  - Provided for simple interactions

```
[
  {
    "action": "get",
    "version": 1,
    "uuid": "1",
    "data": {
      "match": {
        "object": {
          "type": "stream",
          "value": "*"
        },
        "attribute": [
          {
            "opcode": "eq",
            "attribute": "dst-port",
            "type": "signed",
            "value": 443
          },
          {
            "opcode": "eq",
            "attribute": "protocol",
            "type": "signed",
            "value": 6
          }
        ]
      },
      "output": {
        "attributes": [
          "protocol",
          "src-ip",
          "src-reverses",
          "src-port",
          "dst-ip",
          "dst-reverses",
          "dst-port"
        ],
        "minimum-stamp": -3600,
        "maximum-stamp": 0
      }
    }
  }
]
```

Singularity
NETWORKS

The Singularity Networks Solution

Reduce Total Cost of Ownership

- Software Based Solution

  - ***Eliminate Costly Appliance Refresh Cycle***

- Purpose Built Streaming Analytics Database

  - Eliminates Expensive Database Licenses

  - Significantly Reduce Hardware Requirements

Extensible API Driven Platform

- Customize the platform, for the needs of your business.

Q&A
&
Real-time Demo